```
SHOW FILES; DS
File  16:Gale Group PROMT(R) 1990-2003/Nov 21
         (c) 2003 The Gale Group
File  20:Dialog Global Reporter 1997-2003/Nov 24
         (c) 2003 The Dialog Corp.
File  47:Gale Group Magazine DB(TM) 1959-2003/Nov 21
         (c) 2003 The Gale group
File 148:Gale Group Trade & Industry DB 1976-2003/Nov 24
         (c)2003 The Gale Group
File 258:AP News Jul 2000-2003/Nov 24
         (c) 2003 Associated Press
File 262:CBCA Fulltext 1982-2003/Nov
         (c) 2003 Micromedia Ltd.
File 275:Gale Group Computer DB(TM) 1983-2003/Nov 21
         (c) 2003 The Gale Group
File 433:Charleston Newspapers 1997-2003/Nov 22
         (c) 2003 Charleston Newspapers
File 484:Periodical Abs Plustext 1986-2003/Nov W3
         (c) 2003 ProQuest
File 623:Business Week 1985-2003/Nov 21
         (c) 2003 The McGraw-Hill Companies Inc
File 624:McGraw-Hill Publications 1985-2003/Nov 21
         (c) 2003 McGraw-Hill Co. Inc
File 631:Boston Globe 1980-2003/Nov 21
         (c) 2003 Boston Globe

Set     Items   Description
S1         29   ENCRYPTION AND (SUBATOMIC? OR "SUB-ATOMIC") AND ("BLACK-BO-
              X" OR BLACK? OR BLACKBOX)
S2         17   RD (unique items)
S3          0   HOWFILES
?
```

2/9/1 (Item 1 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)

10607020 Supplier Number: 105640905 (THIS IS THE FULLTEXT)

BBN, MagiQ Pioneer U.S. Fiber Encryption Techniques.

Fiber Optics News, v23, n28, p0
July 21, 2003
ISSN: ISSN: 8756-2049
Language: English Record Type: Fulltext
Document Type: Newsletter; Trade
Word Count: 683

TEXT:

Quantum encryption. The term is so new that it isn't even included in the 18th Edition of Newton's Telecom Dictionary, but it has permeated the realms of research and academia. According to the Institute of Optics in Orsay, France, by encoding messages using the quantum states of photons, quantum cryptography offers the prospect of completely secure data transmission.

Researchers at Boston's BBN Corp. are working on an encryption system that eventually could use subatomic particles safeguard voice and data transmission over fiber-optic networks. The research so far involves commercially available lasers and detectors that reportedly emit and detect single photons or pairs of photons, the backbone of quantum cryptography. If this experimentation pans out, BBN's version of quantum cryptography could be important to the future of financial and government communications as a way to thwart hackers, corporate spies or those who just want to disrupt the system.

The 50-year-old BBN was the force behind the ARPANET along with taking credit for the first packet switch, the first router, and the first person-to-person network e-mail. Headquartered in Cambridge, Mass., it touts itself as being "Cambridge's Third University," behind MIT and Harvard University. Its customers are mostly military-based, including the U.S. Department of Defense, the Defense Advanced Research Projects Agency (DARPA), the Defense Logistics Agency and most of the research facilities connected to the country's military services. However, it also has worked with such commercial entities as Mercedes Benz, ITT and Motorola.

The DoD is backing several quantum cryptography experiments as part of a $20.6 million quantum information initiative at DARPA. Under DARPA sponsorship and in partnership with Harvard and Boston University, BBN says it is building the world's first quantum key distribution (QKD) network that uses lasers and photo detectors to send light in such a way as to detect any sort of eavesdropping; via fiber-optic cable, cryptographic keys can encrypt and decrypt a voice or data message. This test network a test network will allow several parties use a fiber-optic cable loop secured by quantum cryptography. BBR says its work is focused on three areas:

* Building a network based on the fundamental principles of quantum physics fully compatible with the current and future Internet arena. This will require the design and development of new hardware, software, and network protocols.
* Increasing both the speed and security of network data transmission by using high-speed sources of entangled photons.
* Identifying the potential problems and vulnerabilities posed by the most sophisticated of hacking techniques and integrating the appropriate safeguards.

So far, experiments at Los Alamos National Laboratory using BBN techniques have shown that photon detectors can pick up a single photon shot through the air, which could bode well for the future securing of satellite transmissions, and the commercial marketplace for quantum cryptography could hit $200 million in the near future.

MagiQ Technologies, founded in 1999, is a privately held company headquartered in New York City with research & development laboratories in Somerville, Mass. Earlier this year, it unveiled a beta version of its

Navaho encryptio[redacted]ystem, touting its "keys" as [redacted]g virtually unhackable. Magiq's Navaho link consists of two black boxes connected by a 30-km fiber-optic link.

MagiQ is quick to say its QKD doesn't replace existing encryption technologies like Secure Socket Layer and the Public Key Infrastructure. Its Navajo will ship with triple DES and AES data encryption as a part of the feature set. And it won't be cheap. MagiQ's quantum cryptography equipment reportedly goes for a hefty $50,000 each. Even so, NEON Communications, a facilities-based wholesale communications provider in Boston that supplies endto-end services in a 12-state northeast and mid-Atlantic region, has tested MagiQ's gear, coming away with a positive feeling.

>> Steve Milligan, BBN, 617/873-8000; Alexei Trifonov, 646/638-1001, ext. 11<<

PUBLISHER NAME: PBI Media, LLC
COMPANY NAMES: *BBN Corp.
DESCRIPTORS: *High technology industry
GEOGRAPHIC NAMES: *1USA (United States)
INDUSTRY NAMES: BUSN (Any type of business); ELEC (Electronics); TELC (Telecommunications)
TICKER SYMBOLS: BBN
?

2/9/4 (Item 1 from file: 258)
DIALOG(R)File 258:AP News Jul

02798305 (THIS IS THE FULLTEXT)
Encryption revolution: the tantalizing promise of `unbreakable' codes
Associated Press
Monday, November 17, 2003 20:52 EST
JOURNAL CODE: AP LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT
DOCUMENT TYPE: NEWSWIRE
WORD COUNT: 932

TEXT:
By BRIAN BERGSTEIN
AP Technology Writer

NEW YORK (AP) - Code-makers could be on the verge of winning their ancient arms race with code-breakers.

After 20 years of research, an encryption process is emerging that is considered unbreakable because it employs the mind-blowing laws of quantum physics.

This month, a small startup called MagiQ Technologies Inc. began selling what appears to be the first commercially available system that uses individual photons to transfer the numeric keys that are widely used to encode and read secret documents.

Photons, discrete particles of energy, are so sensitive that if anyone tries to spy on their travel from one point to another, their behavior will change, tipping off the sender and recipient and invalidating the stolen code.

``There are really no ways (of) cracking this code," said Lov Grover, a quantum computing researcher at Bell Laboratories who is not involved with MagiQ.

Called Navajo -- a nod to the American Indian code specialists of World War II -- MagiQ's system consists of 19-inch black boxes that generate and read the signals over a fiber-optic line.

MagiQ (pronounced ``magic," with the ``Q" for ``quantum") expects that with a cost of $50,000 to $100,000, Navajo will appeal to banks, insurers, government agencies, pharmaceutical companies and other organizations that transmit sensitive information.

``We think this is going to have a huge, positive impact on the world," said Bob Gelfond, MagiQ's founder and chief executive.

Encryption schemes commonly used now are considered safe, though they theoretically could be broken someday.

But even before that day arrives, Gelfond believes quantum encryption is superior in one important way. In some super-high-security settings, people sharing passwords and other information must have the same key, a massive string of digits used to encode data. Sometimes the keys will be transferred by imperfect means -- via courier or special software. They are not changed very often and can be susceptible to interception.

``Even if you have the perfect encryption algorithm, if someone gets your key, you're in trouble," Gelfond said.

The Navajo sys[redacted] not only transmits the keys [redacted] snoop-proof photons, it also changes them 10 times a second. ``Even if somebody could get a copy of the key, it wouldn't do them any good," Gelfond said.

Of course, unbreakable codes would neutralize the ability of intelligence agents to intercept and read messages. That would necessitate greater reliance on human intelligence.

So does the world's foremost code-making and code-breaking organization, the U.S. National Security Agency, worry about the spread of quantum encryption? Better yet, is the NSA using the technology itself? Like most things about the NSA, those answers remain secret.

MagiQ is seeking the government's approval to sell Navajo boxes overseas. Gelfond hopes officials have realized -- after trying and failing to restrict encryption exports in the 1990s -- that there's little point in trying to ``put the genie back in the bottle" once encryption methods have been invented. After all, he said, researchers in China are known to have experimented with quantum encryption.

At least one other company, Switzerland-based id Quantique SA, has produced a system similar to Navajo, though that remains in pilot phase.

Meanwhile, other organizations are exploring different ways of using subatomic particles as code carriers. QinetiQ, the commercial arm of Britain's defense research agency, and the national lab in Los Alamos, New Mexico, have experimented with transmitting quantum keys through the air rather than over fiber-optic lines.

Researchers at IBM Corp., where quantum encryption was first demonstrated in the 1980s, are exploring ways to shrink quantum systems so they can plug more efficiently into existing computing and communications networks.

In any incarnation, quantum encryption employs one of the defining discoveries of physics: Heisenberg's Uncertainty Principle, which says subatomic particles exist in multiple possible states at once, however hard as that may be to imagine, until something interacts with them.

When one Navajo box sends out a code key, it imparts certain measurable characteristics to photons that travel through the fiber-optic line. When the second Navajo box measures those characteristics, that mere act throws off other characteristics -- but the Navajo boxes confer with each other after the transmission is complete and sort it all out. The boxes can be up to 70 miles (112 kilometers) apart, after which additional boxes are needed as relays.

``It's intriguing," said James Capuano, operations director for NEON Communications Inc., a Massachusetts-based telecom carrier that has tested Navajo boxes on its network and now is exploring whether its customers would pay extra to use them. ``It's a very simple product to deploy."

It's also just the first step on a deeper quest to use quantum physics.

Within a few decades, scientists hope to use the multiple possible states and interactions of subatomic particles as replacements for the binary 0s and 1s used in computing today. A

quantum computer, [redacted] it comes to pass, would be [redacted] to perform several complex calculations simultaneously, making it exponentially more powerful than today's supercomputers.

Researchers have performed simple calculations with a few particles but are a long way from being able to replicate that in a large quantum soup in a controllable and consistent manner.

In the 1990s, landmark research by Peter Shor of AT&T Labs showed that quantum computers would be powerful enough to crack any code in use today -- except ones generated through quantum cryptography.

So at long last, code writers might be done fighting to stay ahead of code breakers.

``We'll stop this race," said Gr
goire Ribordy, a founder of id
Quantique. ``We'd like to have a system that's forever secure."

On the Net:

http://www.magiqtech.com

http://www.idquantique.com

GEOGRAPHIC NAMES: AMERICAS; NORTH AMERICA; USA
INDUSTRY NAMES: ADVANCED COMPUTERS; COMPUTER HARDWARE; COMPUTER SECURITY; COMPUTERS; SCIENCE; SECURITY
EVENT NAMES: GOVERNMENT; POLITICAL AND PUBLIC AFFAIRS; RESEARCH AND DEVELOPMENT; TECHNOLOGY DEVELOPMENT
?

T S2/FULL/5

2/9/5 (Item 2 from file: 258)
DIALOG(R)File 258:AP News Jul

02794697 (THIS IS THE FULLTEXT)
Encryption Promises Unbreakable Codes
Associated Press
Sunday, November 16, 2003 12:08 EST
JOURNAL CODE: AP LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT
DOCUMENT TYPE: NEWSWIRE
WORD COUNT: 928

TEXT:
By BRIAN BERGSTEIN
AP Technology Writer

NEW YORK (AP) - Code-makers could be on the verge of winning their ancient arms race with code-breakers.

After 20 years of research, an encryption process is emerging that is considered unbreakable because it employs the mind-blowing laws of quantum physics.

This month, a small startup called MagiQ Technologies Inc. began selling what appears to be the first commercially available system that uses individual photons to transfer the numeric keys that are widely used to encode and read secret documents.

Photons, discrete particles of energy, are so sensitive that if anyone tries to spy on their travel from one point to another, their behavior will change, tipping off the sender and recipient and invalidating the stolen code.

``There are really no ways (of) cracking this code," said Lov Grover, a quantum computing researcher at Bell Laboratories who is not involved with MagiQ.

Called Navajo -- a nod to the American Indian code specialists of World War II -- MagiQ's system consists of 19-inch black boxes that generate and read the signals over a fiber-optic line.

MagiQ (pronounced ``magic," with the ``Q" for ``quantum") expects that with a cost of $50,000 to $100,000, Navajo will appeal to banks, insurers, government agencies, pharmaceutical companies and other organizations that transmit sensitive information.

``We think this is going to have a huge, positive impact on the world," said Bob Gelfond, MagiQ's founder and chief executive.

Encryption schemes commonly used now are considered safe, though they theoretically could be broken someday.

But even before that day arrives, Gelfond believes quantum encryption is superior in one important way. In some super-high-security settings, people sharing passwords and other information must have the same key, a massive string of digits used to encode data. Sometimes the keys will be transferred by imperfect means -- via courier or special software. They are not changed very often and can be susceptible to interception.

``Even if you have the perfect encryption algorithm, if someone gets your key, you're in trouble," Gelfond said.

The Navajo sys[redacted] not only transmits the keys [redacted] hoop-proof photons, it also changes them 10 times a second. "Even if somebody could get a copy of the key, it wouldn't do them any good," Gelfond said.

Of course, unbreakable codes would neutralize the ability of intelligence agents to intercept and read messages. That would necessitate greater reliance on human intelligence.

So does the world's foremost code-making and code-breaking organization, the U.S. National Security Agency, worry about the spread of quantum encryption? Better yet, is the NSA using the technology itself? Like most things about the NSA, those answers remain secret.

MagiQ is seeking the government's approval to sell Navajo boxes overseas. Gelfond hopes officials have realized -- after trying and failing to restrict encryption exports in the 1990s -- that there's little point in trying to ``put the genie back in the bottle" once encryption methods have been invented. After all, he said, researchers in China are known to have experimented with quantum encryption.

At least one other company, Switzerland-based id Quantique SA, has produced a system similar to Navajo, though that remains in pilot phase.

Meanwhile, other organizations are exploring different ways of using subatomic particles as code carriers. QinetiQ, the commercial arm of Britain's defense research agency, and the national lab in Los Alamos, N.M., have experimented with transmitting quantum keys through the air rather than over fiber-optic lines.

Researchers at IBM Corp., where quantum encryption was first demonstrated in the 1980s, are exploring ways to shrink quantum systems so they can plug more efficiently into existing computing and communications networks.

In any incarnation, quantum encryption employs one of the defining discoveries of physics: Heisenberg's Uncertainty Principle, which says subatomic particles exist in multiple possible states at once, however hard as that may be to imagine, until something interacts with them.

When one Navajo box sends out a code key, it imparts certain measurable characteristics to photons that travel through the fiber-optic line. When the second Navajo box measures those characteristics, that mere act throws off other characteristics -- but the Navajo boxes confer with each other after the transmission is complete and sort it all out. The boxes can be up to 70 miles apart, after which additional boxes are needed as relays.

``It's intriguing," said James Capuano, operations director for NEON Communications Inc., a Massachusetts-based telecom carrier that has tested Navajo boxes on its network and now is exploring whether its customers would pay extra to use them. ``It's a very simple product to deploy."

It's also just the first step on a deeper quest to use quantum physics.

Within a few decades, scientists hope to use the multiple possible states and interactions of subatomic particles as replacements for the binary 0s and 1s used in computing today. A quantum computer, if it comes to pass, would be able to perform

several complex c[redacted]ulations simultaneously, maki[redacted]t exponentially more powerful than today's supercomputers.

Researchers have performed simple calculations with a few particles but are a long way from being able to replicate that in a large quantum soup in a controllable and consistent manner.

In the 1990s, landmark research by Peter Shor of AT&T Labs showed that quantum computers would be powerful enough to crack any code in use today -- except ones generated through quantum cryptography.

So at long last, code writers might be done fighting to stay ahead of code breakers.

``We'll stop this race," said Gregoire Ribordy, a founder of id Quantique. ``We'd like to have a system that's forever secure."

On the Net:

http://www.magiqtech.com

http://www.idquantique.com

INDUSTRY NAMES: ADVANCED COMPUTERS; COMPUTER HARDWARE; COMPUTER SECURITY; COMPUTERS; SCIENCE; SECURITY
EVENT NAMES: GOVERNMENT; POLITICAL AND PUBLIC AFFAIRS; RESEARCH AND DEVELOPMENT; TECHNOLOGY DEVELOPMENT
?

2/9/10 (Item 1 from file: 623)

DIALOG(R)File 623:Business Week

00776800 (THIS IS THE FULLTEXT)

A Quantum Leap in Cryptography: Visionaries are using photons to develop data-security systems that may prove the ultimate defense against eavesdropping hackers

Business Week Online, July 15, 2003, 20030715, Pg 0
JOURNAL CODE: BWON
SECTION HEADING: Technology
WORD COUNT: 1,226

TEXT: In a dark, quiet room inside the Boston labs of BBN Corp. (VZ), network engineer Chip Elliott is using the laws of physics to build what he hopes will be an unbreakable encryption machine. The system, which sits atop a pink heat-absorption table, is designed to harness subatomic particles to create a hacker-proof way to communicate over fiber-optic networks.

To build his black box, Elliott has used off-the-shelf fiber-optic gear such as lasers and detectors, which he has tweaked to do unusual things. The goal is to reliably emit and detect single photons or tightly linked pairs of photons -- the key particles in light waves. It's all part of a leading edge information-security field known as quantum cryptography. Over the next few years, Elliott and others in the field may turn the information-security business on its ear. Quantum cryptography could make the secret codes that protect data transmissions far more difficult to decipher -- an important feature for financial-services companies, telecom carriers, and governments. Quantum cryptography may also quickly alert systems administrators to the presence of cybersnoops, whether they be hackers, fraudsters, or corporate spies.

OBSERVED -- AND ALTERED. In theory, that will all be thanks to Heisenberg's Uncertainty Principle. This basic law of physics, postulated in 1927 by German physicist Werner Heisenberg, holds that the mere act of observing or measuring a particle will ultimately change its behavior. At macroscopic levels, humans don't notice this law. Put your leg inside an MRI machine, for example, and it doesn't come out noticeably different. But at the atomic level, the MRI's application of strong magnetic forces alters the trajectory and spin of the electrons that are orbiting atoms inside your body.

Messing with photons in a data stream will have the same effect. Under the laws of quantum physics, a moving photon has one of four orientations; vertical, horizontal, or diagonal in opposing directions. Lasers can be modified to emit single photons, each possessing a particular orientation. Photon detectors -- such as a hacker might use -- can record that orientation. But according to Heisenberg's principle, doing so will change the orientation of some particles. That will tip off the sender and the receiver, who can reencode their transmission or switch to a different communications line to avoid eavesdroppers.

Scientists have been working on the concepts behind quantum cryptography for three decades. After a long journey from chalkboard to lab to working prototype, the field is on the verge of a breakout. A Swiss firm, ID Quantique, introduced the first commercial quantum cryptography products last summer. Sometime this summer, MagiQ Technologies in New York City is expected to unveil its Navajo quantum cryptographic system. Several communications companies are currently testing Navajo on their networks, and researchers in the field say the U.S. government could already be using quantum cryptography to secure communications.

IN THE LOOP. In fact, the Defense Dept. is funding numerous quantum cryptography experiments as part of its $20.6 million quantum information initiative at the Defense Advance Research Projects Agency (DARPA). MagiQ estimates that the market for quantum cryptography will hit $200 million within the next few years. It sells its quantum cryptography units for

$50,000 apiece.
BBN, meantime, is building a test network funded by DARPA that will allow multiple parties to tap into a fiber-optic cable loop secured by quantum cryptography. "Rather than having one link protected by quantum cryptography, we imagined a big service where everyone could connect to everybody else," explains Elliot. And at Los Alamos National Laboratory in New Mexico, quantum cryptography researcher Richard Hughes already has run experiments proving that photon detectors can pick up a single photon shot through the air. This could ultimately lead to a role for quantum cryptography in securing satellite communications.
And yet quantum cryptography remains an immature technology. Researchers have only been able to send photon signals for limited distances -- 100 kilometers or less -- over fiber optic cables. Photon detectors aren't particularly reliable, either. They often signal that they've detected a photon when one never arrived. "As much as possible, you want to suppress spurious signals," explains Donald Bethune, a quantum cryptography and photonics expert at IBM's (IBM) Almaden Research Center. "Just having the detector running in an environment that's too warm can cause this problem." To some degree, scientists can compensate for such flakiness with super-cooled detectors and error-correction software that can sift through the noise and pick out the valid signals.
STOLEN KEYS. Another problem, for now, is that bursts of single photons move too slowly to be an effective means of real-time data exchange. Once errors are factored in, most quantum encryption systems move data at a rate of 1,000 bits per second or less. This is 1/10,000 the transmission speed of today's fastest systems. For that reason, MagiQ and ID Quantique hope to use quantum cryptography initially to securely distribute secret numerical keys. Nearly ubiquitous in computer security today, these keys are required to decode data encrypted by traditional means -- using mathematical equations to obscure the plain text of messages.
Key distribution has long been a weak link of digital encryption. Hackers who get their hands on secret encryption keys can intercept and read a data stream without the violated parties finding out. "Digital keys can be copied with 100% fidelity and an insider could sell the key to a criminal or some corporate espionage operative and create a vulnerability in the data being transmitted," says Robert Gelfond, CEO of MagiQ.
A key distributed via quantum cryptography, however, would be all but impossible to steal. If a bank pairs a quantum cryptography system with a classical encryption system, then the quantum unit can be automated to pass fresh, secret keys from the sender to the receiver with assurance that no one has read those keys. It can do so as often as several times a second without slowing the data transmission. Since the key exchange is automated with quantum crypto, it's also much easier to work with than existing key-exchange mechanisms, which require more human intervention.
SIMPLE TO USE. None of this will matter if an enterprising hacker has put a keyboard-sniffer program on your machine to detect your keystrokes. Still, quantum cryptography will provide a new layer of safety for whom paranoia is an essential fact of life -- the kind of people who inhabit banks and the Defense Dept. While the concept and execution of quantum cryptography remain complex, apparently the technology, even it is immature state, is ready for prime time.
Jim Capuano is the operations director at NEON Communications, a Boston-based fiber-optic bandwidth retailer with 80 major customers along the Northeast Corridor. His company test-drove MagiQ's system earlier this spring, and he came away impressed. "It's a very simple product to configure," says Capuano. ID Quantique likewise has customers up and running on its system. The computer world just might be witnessing a new and intriguing phase in the history of cybersecurity.<byline>
By Alex Salkever

COMPANY NAMES (DIALOG GENERATED): Almaden Research Center ; BBN Corp ; Defense Advance Research Projects Agency ; IBM ; ID Quantique ; Los Alamos National Laboratory ; MagiQ Technologies ; NEON Communications ; Quantum ; VZ

?

T S2/3,KWIC/1,4,5[redacted],14,16,17

2/3,KWIC/1 (Item 1 from file: 16)
DIALOG(R)File 16:Gale Group PROMT(R)

10607020 Supplier Number: 105640905 (USE FORMAT 7 FOR FULLTEXT)
BBN, MagiQ Pioneer U.S. Fiber Encryption Techniques.
Fiber Optics News, v23, n28, p0
July 21, 2003
Language: English Record Type: Fulltext
Document Type: Newsletter; Trade
Word Count: 683

(USE FORMAT 7 FOR FULLTEXT)
BBN, MagiQ Pioneer U.S. Fiber Encryption Techniques.
TEXT:
Quantum encryption . The term is so new that it isn't even included in the 18th Edition...

Researchers at Boston's BBN Corp. are working on an encryption system that eventually could use subatomic particles safeguard voice and data transmission over fiber-optic networks. The research so far involves ...laboratories in Somerville, Mass. Earlier this year, it unveiled a beta version of its Navaho encryption system, touting its "keys" as being virtually unhackable. Magiq's Navaho link consists of two black boxes connected by a 30-km fiber-optic link.

MagiQ is quick to say its QKD doesn't replace existing encryption technologies like Secure ...and the Public Key Infrastructure. Its Navajo will ship with triple DES and AES data encryption as a part of the feature set. And it won't be cheap. MagiQ's...

2/3,KWIC/4 (Item 1 from file: 258)
DIALOG(R)File 258:AP News Jul

02798305 (USE FORMAT 7 FOR FULLTEXT)
Encryption revolution: the tantalizing promise of `unbreakable' codes
Associated Press
Monday, November 17, 2003 20:52 EST
JOURNAL CODE: AP LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT
DOCUMENT TYPE: NEWSWIRE
WORD COUNT: 932

Encryption revolution: the tantalizing promise of `unbreakable' codes

TEXT:
...of winning
their ancient arms race with code-breakers.

After 20 years of research, an encryption process is emerging that is considered unbreakable because it employs the mind-blowing laws of...

...American Indian code specialists of
World War II -- MagiQ's system consists of 19-inch black boxes that generate and read the signals over a fiber-optic line.

MagiQ (pronounced ``magic...

...huge, positive impact on the
world," said Bob Gelfond, MagiQ's founder and chief executive.

Encryption schemes commonly used now are considered safe, though

they theoretically could be broken someday.

But even before that day arrives, Gelfond believes quantum encryption is superior in one important way. In some super-high-security settings, people sharing passwords...

...changed very
often and can be susceptible to interception.

``Even if you have the perfect encryption algorithm, if someone gets your key, you're in trouble," Gelfond said.
The Navajo system...

...code-breaking
organization, the U.S. National Security Agency, worry about the spread of quantum encryption ? Better yet, is the NSA using the technology itself? Like most things about the NSA...

...sell Navajo boxes
overseas. Gelfond hopes officials have realized -- after trying and failing to restrict encryption exports in the 1990s -- that there's little point in trying to ``put the genie back in the bottle" once encryption methods have been invented. After all, he said, researchers in China are known to have experimented with quantum encryption .

At least one other company, Switzerland-based id Quantique SA, has produced a system similar...

...though that remains in
pilot phase.

Meanwhile, other organizations are exploring different ways of using subatomic particles as code carriers. QinetiQ, the commercial arm of Britain's defense research agency, and...

...through the air rather than over fiber-optic lines.

Researchers at IBM Corp., where quantum encryption was first demonstrated in the 1980s, are exploring ways to shrink quantum systems so they can plug more efficiently into existing computing and communications networks.

In any incarnation, quantum encryption employs one of the defining discoveries of physics: Heisenberg's Uncertainty Principle, which says subatomic particles exist in multiple possible states at once, however hard as that may be to...

...Within a few decades, scientists hope to use the multiple possible states and interactions of subatomic particles as replacements for the binary 0s and 1s used in computing today. A quantum...

2/3,KWIC/5 (Item 2 from file: 258)
DIALOG(R)File 258:AP News Jul

02794697 (USE FORMAT 7 FOR FULLTEXT)
Encryption Promises Unbreakable Codes
Associated Press
Sunday, November 16, 2003 12:08 EST
JOURNAL CODE: AP LANGUAGE: ENGLISH RECORD TYPE: FULLTEXT
DOCUMENT TYPE: NEWSWIRE
WORD COUNT: 928

Encryption Promises Unbreakable Codes

TEXT:
...of winning
their ancient arms race with code-breakers.

After 20 years of research, an encryption process is emerging that is considered unbreakable because it employs the mind-blowing laws of...

...American Indian code specialists of
World War II -- MagiQ's system consists of 19-inch black boxes that generate and read the signals over a fiber-optic line.

MagiQ (pronounced ``magic...

...huge, positive impact on the
world," said Bob Gelfond, MagiQ's founder and chief executive.

Encryption schemes commonly used now are considered safe, though they theoretically could be broken someday.

But even before that day arrives, Gelfond believes quantum encryption is superior in one important way. In some super-high-security settings, people sharing passwords...

...changed very
often and can be susceptible to interception.

``Even if you have the perfect encryption algorithm, if someone gets your key, you're in trouble," Gelfond said.
The Navajo system...

...code-breaking
organization, the U.S. National Security Agency, worry about the spread of quantum encryption ? Better yet, is the NSA using the technology itself? Like most things about the NSA...

...sell Navajo boxes
overseas. Gelfond hopes officials have realized -- after trying and failing to restrict encryption exports in the 1990s -- that there's little point in trying to ``put the genie back in the bottle" once encryption methods have been invented. After all, he said, researchers in China are known to have experimented with quantum encryption .

At least one other company, Switzerland-based id Quantique SA, has produced a system similar...

...though that remains in
pilot phase.

Meanwhile, other organizations are exploring different ways of using subatomic particles as code carriers. QinetiQ, the commercial arm of Britain's defense research agency, and...

...through the air rather than over fiber-optic lines.

Researchers at IBM Corp., where quantum encryption was first demonstrated in the 1980s, are exploring ways to shrink quantum systems so they can plug more efficiently into existing computing and communications networks.

In any incarnation, quantum encryption employs one of the

defining discoveries [redacted] physics: Heisenberg's Uncert[redacted]ty Principle, which says subatomic particles exist in multiple possible states at once, however hard as that may be to...

...Within a few decades, scientists hope to use the multiple possible states and interactions of subatomic particles as replacements for the binary 0s and 1s used in computing today. A quantum...
>>>Item 19 is not within valid item range for file 995
?

2/9/14 (Item 1 from file: 707)
DIALOG(R)File 707:The Seattle Times

12321077

Startup making a quantum leap with encryption Physics provides key to protecting codes

Seattle Times (SE) - Monday November 17, 2003
By: Brian Bergstein; The Associated Press
Edition: Fourth Section: ROP Business Page: C3
Word Count: 935

TEXT:
NEW YORK Code-makers could be on the verge of winning their ancient arms race with code-breakers.

After 20 years of research, an encryption process is emerging that is considered unbreakable because it employs the mind-blowing laws of quantum physics.

This month, a small startup called MagiQ Technologies began selling what appears to be the first commercially available system that uses individual photons to transfer the numeric keys that are widely used to encode and read secret documents.

Photons, discrete particles of energy, are so sensitive that if anyone tries to spy on their travel from one point to another, their behavior will change, tipping off the sender and recipient and invalidating the stolen code.

"There are really no ways (of) cracking this code," said Lov Grover, a quantum computing researcher at Bell Laboratories who is not involved with MagiQ.

Called Navajo a nod to the American Indian "code talkers" who used the Navajo language to send secret messages in World War II MagiQ's system consists of 19-inch black boxes that generate and read the signals over a fiber-optic line.

MagiQ (pronounced "magic," with the "Q" for "quantum") expects that, at a cost of $50,000 to $100,000, Navajo will appeal to banks, insurers, government agencies, pharmaceutical companies and other organizations that transmit sensitive information.

"We think this is going to have a huge, positive impact on the world," said Bob Gelfond, MagiQ's founder and chief executive.

Encryption schemes commonly used now are considered safe, though they theoretically could be broken someday.

But even before that day arrives, Gelfond believes quantum encryption is superior in one important way. In some super-high-security settings, people sharing passwords and other information must have the same key, a massive string of digits used to encode data. Sometimes the keys will be transferred by imperfect means via courier or special software. They are not changed very often and can be susceptible to interception.

"Even if you have the perfect encryption algorithm, if someone gets your key, you're in trouble," Gelfond said.

Constantly changing

The Navajo system not only transmits the keys on snoop-proof photons, it also changes them 10 times a second. "Even if somebody could get a copy of the key, it wouldn't do them any good," Gelfond said.

Of course, unbreakable codes would neutralize the ability of intelligence agents to intercept and read messages. That would necessitate greater reliance on human intelligence.

So does the world's foremost code-making and code-breaking organization, the U.S. National Security Agency, worry about the spread of quantum encryption? Better yet, is the NSA using the technology itself? Like most things about the NSA, those answers remain secret.

MagiQ is seeking the government's approval to sell Navajo boxes overseas. Gelfond hopes officials have realized after trying and failing to restrict encryption exports in the 1990s that there's little point in trying to "put the genie back in the bottle" once encryption methods have been invented. After all, he said, researchers in China are known to have experimented with quantum encryption.

At least one other company, Switzerland-based id Quantique, has produced a system similar to Navajo, though that remains in pilot phase.

Meanwhile, other organizations are exploring different ways of using subatomic particles as code carriers. QinetiQ, the commercial arm of Britain's defense research agency, and the national lab in Los Alamos, N.M., have experimented with transmitting quantum keys through the air rather than over fiber-optic lines.

Researchers at IBM, where quantum encryption was first demonstrated in the 1980s, are exploring ways to shrink quantum systems so they can plug more efficiently into existing computing and communications networks.

In any incarnation, quantum encryption employs one of the defining discoveries of physics: Heisenberg's Uncertainty Principle, which says subatomic particles exist in multiple possible states at once, however hard that may be to imagine, until something interacts with them.

When one Navajo box sends out a code key, it imparts certain measurable characteristics to photons that travel through the fiber-optic line. When the second Navajo box measures those characteristics, that mere act throws off other characteristics but the Navajo boxes confer with each other after the transmission is complete and sort it all out. The boxes can be up to 70 miles apart, after which additional boxes are needed as relays.

Simple and intriguing

"It's intriguing," said James Capuano, operations director for NEON Communications, a Westborough, Mass.-based telecommunications carrier that has tested Navajo boxes on its network and now is exploring whether its customers would pay extra to use them. "It's a very simple product to deploy."

It's also just the first step on a deeper quest to use quantum physics.

Within a few decades, scientists hope to use the multiple possible states and interactions of subatomic particles as replacements for the binary 0s and 1s used in computing today.

A quantum computer, if it comes to pass, would be able to perform several complex calculations simultaneously, making it exponentially more powerful than today's supercomputers.

Researchers have performed simple calculations with a few particles but are a long way from being able to replicate that in a large quantum soup in a controllable and consistent manner.

In the 1990s, landmark research by Peter Shor of AT&T Labs showed that quantum computers would be powerful enough to crack any code in use today except ones generated through quantum cryptography.

CAPTION:
Elise Amendola / The Associated Press : Liu Ping, an electrical engineer for MagiQ Technologies, works at his desk at the Somerville, Mass., startup that makes an encryption process called Navajo using principles of quantum physics. (0393639981)

?

2/9/16 (Item 1 from file: 990)
DIALOG(R)File 990:NewsRoom Current

0733529622 16CV0WXP

New code believed to be unbreakable

Brian Bergstein, The Associated Press
Charleston Gazette (WV), p02C
Monday, November 17, 2003
JOURNAL CODE: ACFN LANGUAGE: English RECORD TYPE: Fulltext
DOCUMENT TYPE: Newspaper SECTION HEADING: News
WORD COUNT: 906

TEXT:
NEW YORK - Code-makers could be on the verge of winning their ancient arms race with code-breakers. After 20 years of research, an encryption process is emerging that is considered unbreakable because it employs the mind-blowing laws of quantum physics.

This month, a small startup called MagiQ Technologies Inc. began selling what appears to be the first commercially available system that uses individual photons to transfer the numeric keys that are widely used to encode and read secret documents.

Photons, discrete particles of energy, are so sensitive that if anyone tries to spy on their travel from one point to another, their behavior will change, tipping off the sender and recipient and invalidating the stolen code.

"There are really no ways [of] cracking this code," said Lov Grover, a quantum computing researcher at Bell Laboratories who is not involved with MagiQ.

Called Navajo - a nod to the American Indian code specialists of World War II - MagiQ's system consists of 19-inch black boxes that generate and read the signals over a fiber-optic line.

MagiQ (pronounced "magic," with the "Q" for "quantum") expects that with a cost of $50,000 to $100,000, Navajo will appeal to banks, insurers, government agencies, pharmaceutical companies and other organizations that transmit sensitive information.

"We think this is going to have a huge, positive impact on the world," said Bob Gelfond, MagiQ's founder and chief executive.

Encryption schemes commonly used now are considered safe, though they theoretically could be broken someday.
But even before that day arrives, Gelfond believes quantum encryption is superior in one important way. In some super-high-security settings, people sharing passwords and other information must have the same key, a massive string of digits used to encode data. Sometimes the keys will be transferred by imperfect means - via courier or special software. They are not changed very often and can be susceptible to interception.

"Even if you have the perfect encryption algorithm, if someone gets your key, you're in trouble," Gelfond said.

The Navajo system not only transmits the keys on snoop-proof photons; it also changes them 10 times a second. "Even if somebody could get a copy of the key, it wouldn't do them any good," Gelfond said.

Of course, unbreakable codes would neutralize the ability of intelligence agents to intercept and read messages. That would necessitate greater

reliance on human [redacted]telligence.

So does the world's foremost code-making and code-breaking organization, the U.S. National Security Agency, worry about the spread of quantum encryption? Better yet, is the NSA using the technology itself? Like most things about the NSA, those answers remain secret.
MagiQ is seeking the government's approval to sell Navajo boxes overseas. Gelfond hopes officials have realized - after trying and failing to restrict encryption exports in the 1990s - that there's little point in trying to "put the genie back in the bottle" once encryption methods have been invented. After all, he said, researchers in China are known to have experimented with quantum encryption.

At least one other company, Switzerland-based id Quantique SA, has produced a system similar to Navajo, though that remains in pilot phase.

Meanwhile, other organizations are exploring different ways of using subatomic particles as code carriers. QinetiQ, the commercial arm of Britain's defense research agency, and the national lab in Los Alamos, N.M., have experimented with transmitting quantum keys through the air rather than over fiber-optic lines.

Researchers at IBM Corp., where quantum encryption was first demonstrated in the 1980s, are exploring ways to shrink quantum systems so they can plug more efficiently into existing computing and communications networks.

In any incarnation, quantum encryption employs one of the defining discoveries of physics: Heisenberg's Uncertainty Principle, which says subatomic particles exist in multiple possible states at once, however hard as that may be to imagine, until something interacts with them.

When one Navajo box sends out a code key, it imparts certain measurable characteristics to photons that travel through the fiber-optic line. When the second Navajo box measures those characteristics, that mere act throws off other characteristics - but the Navajo boxes confer with each other after the transmission is complete and sort it all out. The boxes can be up to 70 miles apart, after which additional boxes are needed as relays.

"It's intriguing," said James Capuano, operations director for NEON Communications Inc., a Massachusetts-based telecom carrier that has tested Navajo boxes on its network and now is exploring whether its customers would pay extra to use them. "It's a very simple product to deploy."

It's also just the first step on a quest to use quantum physics.

Within a few decades, scientists hope to use the multiple possible states and interactions of subatomic particles as replacements for the binary 0s and 1s used in computing today. A quantum computer, if it comes to pass, would be able to perform several complex calculations simultaneously, making it exponentially more powerful than today's supercomputers. Researchers have performed simple calculations with a few particles but are a long way from being able to replicate that in a large quantum soup in a controllable and consistent manner.

In the 1990s, landmark research by Peter Shor of AT&T Labs showed that quantum computers would be powerful enough to crack any code in use today - except ones generated through quantum cryptography.

COMPANY NAMES: AT AND T BELL LABORATORIES; AT AND T BELL LABORATORIES; INTERNATIONAL BUSINESS MACHINES; MAGIQ TECHNOLOGIES; NEON COMMUNICATIONS; QUANTIQUE; US NATIONAL SECURITY AGENCY; INTERNATIONAL BUSINESS MACHINES CORP; T LABS LLC
EVENT NAMES: GOVERNMENT; POLITICAL AND PUBLIC AFFAIRS; RESEARCH AND

DEVELOPMENT; TECHNOLOGY DEVELOPMENT
GEOGRAPHIC NAMES: AMERICAS; NORTH AMERICA; USA
INDUSTRY NAMES: ADVANCED COMPUTERS; COMPUTER HARDWARE; COMPUTERS; SCIENCE; SECURITY
JOURNAL REGION: West Virginia; USA
JOURNAL SUBJECT: General News
?

T S2/FULL/17

2/9/17 (Item 2 from file: 990)
DIALOG(R)File 990:NewsRoom Current

0733528724 16CV0W1M

Encryption revolution: the tantalizing promise of `unbreakable' codes

BRIAN BERGSTEIN AP Technology Writer
AP Worldstream
Monday, November 17, 2003
JOURNAL CODE: APTK LANGUAGE: English RECORD TYPE: Fulltext
DOCUMENT TYPE: Newswire
WORD COUNT: 962

TEXT:
NEW YORK (AP) _ Code-makers could be on the verge of winning their ancient arms race with code-breakers.

After 20 years of research, an encryption process is emerging that is considered unbreakable because it employs the mind-blowing laws of quantum physics.

This month, a small startup called MagiQ Technologies Inc. began selling what appears to be the first commercially available system that uses individual photons to transfer the numeric keys that are widely used to encode and read secret documents.
Photons, discrete particles of energy, are so sensitive that if anyone tries to spy on their travel from one point to another, their behavior will change, tipping off the sender and recipient and invalidating the stolen code.

"There are really no ways (of) cracking this code," said Lov Grover, a quantum computing researcher at Bell Laboratories who is not involved with MagiQ.

Called Navajo _ a nod to the American Indian code specialists of World War II _ MagiQ's system consists of 19-inch black boxes that generate and read the signals over a fiber-optic line.

MagiQ (pronounced "magic," with the "Q" for "quantum") expects that with a cost of $50,000 to $100,000, Navajo will appeal to banks, insurers, government agencies, pharmaceutical companies and other organizations that transmit sensitive information.

"We think this is going to have a huge, positive impact on the world," said Bob Gelfond, MagiQ's founder and chief executive.

Encryption schemes commonly used now are considered safe, though they theoretically could be broken someday.

But even before that day arrives, Gelfond believes quantum encryption is superior in one important way. In some super-high-security settings, people sharing passwords and other information must have the same key, a massive string of digits used to encode data. Sometimes the keys will be transferred by imperfect means _ via courier or special software. They are not changed very often and can be susceptible to interception.

"Even if you have the perfect encryption algorithm, if someone gets your key, you're in trouble," Gelfond said.

The Navajo system not only transmits the keys on snoop-proof photons, it also changes them 10 times a second. "Even if somebody could get a copy of the key, it wouldn't do them any good," Gelfond said.

Of course, unbreakable codes would neutralize the ability of intelligence agents to intercept and read messages. That would necessitate greater reliance on human intelligence.

So does the world's foremost code-making and code-breaking organization, the U.S. National Security Agency, worry about the spread of quantum encryption? Better yet, is the NSA using the technology itself? Like most things about the NSA, those answers remain secret.

MagiQ is seeking the government's approval to sell Navajo boxes overseas. Gelfond hopes officials have realized _ after trying and failing to restrict encryption exports in the 1990s _ that there's little point in trying to "put the genie back in the bottle" once encryption methods have been invented. After all, he said, researchers in China are known to have experimented with quantum encryption.

At least one other company, Switzerland-based id Quantique SA, has produced a system similar to Navajo, though that remains in pilot phase.

Meanwhile, other organizations are exploring different ways of using subatomic particles as code carriers. QinetiQ, the commercial arm of Britain's defense research agency, and the national lab in Los Alamos, New Mexico, have experimented with transmitting quantum keys through the air rather than over fiber-optic lines.

Researchers at IBM Corp., where quantum encryption was first demonstrated in the 1980s, are exploring ways to shrink quantum systems so they can plug more efficiently into existing computing and communications networks.
In any incarnation, quantum encryption employs one of the defining discoveries of physics: Heisenberg's Uncertainty Principle, which says subatomic particles exist in multiple possible states at once, however hard as that may be to imagine, until something interacts with them.

When one Navajo box sends out a code key, it imparts certain measurable characteristics to photons that travel through the fiber-optic line. When the second Navajo box measures those characteristics, that mere act throws off other characteristics _ but the Navajo boxes confer with each other after the transmission is complete and sort it all out. The boxes can be up to 70 miles (112 kilometers) apart, after which additional boxes are needed as relays.

"It's intriguing," said James Capuano, operations director for NEON Communications Inc., a Massachusetts-based telecom carrier that has tested Navajo boxes on its network and now is exploring whether its customers would pay extra to use them. "It's a very simple product to deploy."

It's also just the first step on a deeper quest to use quantum physics.

Within a few decades, scientists hope to use the multiple possible states and interactions of subatomic particles as replacements for the binary 0s and 1s used in computing today. A quantum computer, if it comes to pass, would be able to perform several complex calculations simultaneously, making it exponentially more powerful than today's supercomputers.

Researchers have performed simple calculations with a few particles but are a long way from being able to replicate that in a large quantum soup in a controllable and consistent manner.

In the 1990s, landmark research by Peter Shor of AT&T Labs showed that quantum computers would be powerful enough to crack any code in use today _ except ones generated through quantum cryptography.

So at long last, code writers might be done fighting to stay ahead of code breakers.

"We'll stop this rac[redacted] said Gr goire Ribordy, a fou[redacted] of id Quantique. "We'd like to have a system that's forever secure."

On the Net:
http://www.magiqtech.com

http://www.idquantique.com

COMPANY NAMES: BELL LABORATORIES; INTERNATIONAL BUSINESS MACHINES CORP; NEON COMMUNICATIONS; T LABS LLC
EVENT NAMES: GOVERNMENT; POLITICAL AND PUBLIC AFFAIRS; RESEARCH AND DEVELOPMENT; TECHNOLOGY DEVELOPMENT
GEOGRAPHIC NAMES: AMERICAS; NORTH AMERICA; USA
INDUSTRY NAMES: ADVANCED COMPUTERS; COMPUTER HARDWARE; COMPUTER SECURITY; COMPUTERS; SCIENCE; SECURITY
JOURNAL REGION: USA
JOURNAL SUBJECT: General News
?